CLAIMS

What is claimed is:

1. A method comprising:

implementing a virtual machine monitor upon a computing system having a native environment that executes in physical mode; and

executing the virtual machine monitor in a most privileged mode, the virtual machine monitor emulating physical mode such that the native environment is executed in a less privileged mode.

2. The method of claim 1 wherein the native environment is selected from the list including a 32-bit environment, a 64- bit environment, and a PC/AT environment.

3. The method of claim 2 wherein the VMM contains code to provide functionality selected from the list consisting of PC/AT hardware emulation, PC/AT environment emulation, secure storage, and secure execution.

4. The method of claim 3 wherein the secure storage is used to store security-related information.

5. The method of claim 4 wherein the security-related information is signature authentication and encrypted hash information.

6. The method of claim 5 wherein the security related information is used to create attestation logs.

7. A method comprising:

implementing a virtual machine monitor on a computing system having an extensible firmware architecture such that untrusted code is executed in sandbox mode such that the code is prevented from harming the system.

8. The method of claim 7 wherein the code is legacy BIOS code.

9. A machine-readable medium that provides executable instructions which, when executed by a processor, cause the processor to perform a method, the method comprising:

implementing a virtual machine monitor upon a computing system having a native environment that executes in physical mode; and

executing the virtual machine monitor in a most privileged mode, the virtual machine monitor emulating physical mode such that the native environment is executed in a less privileged mode.

10. The machine-readable medium of claim 9 wherein the native environment is selected from the list including a 32-bit environment, a 64- bit environment, and a PC/AT environment.

11. The machine-readable medium of claim 10 wherein the VMM contains code to provide functionality selected from the list consisting of PC/AT hardware emulation, PC/AT environment emulation, secure storage, and secure execution.

12. The machine-readable medium of claim 11 wherein the secure storage is used to store security-related information.

13. The machine-readable medium of claim 12 wherein the security-related information is signature authentication and encrypted hash information.

14. The machine-readable medium of claim 13 wherein the security related information is used to create attestation logs.

15. An apparatus comprising:

a computing system having a native execution environment that executes in physical mode; and

a virtual machine monitor, executed in a most privileged mode, implemented thereon, the virtual machine monitor emulating physical mode such that the native environment is executed in a less privileged mode.

16. The apparatus of claim 15 wherein the native environment is selected from the list including a 32-bit environment, a 64- bit environment, and a PC/AT environment.

17. The apparatus of claim 16 wherein the VMM contains code to provide functionality selected from the list consisting of PC/AT hardware emulation, PC/AT environment emulation, secure storage, and secure execution.

18. The apparatus of claim 17 wherein the secure storage is used to store security-related information.

19. The apparatus of claim 18 wherein the security-related information is signature authentication and encrypted hash information.

20. The apparatus of claim 19 wherein the security related information is used to create attestation logs.